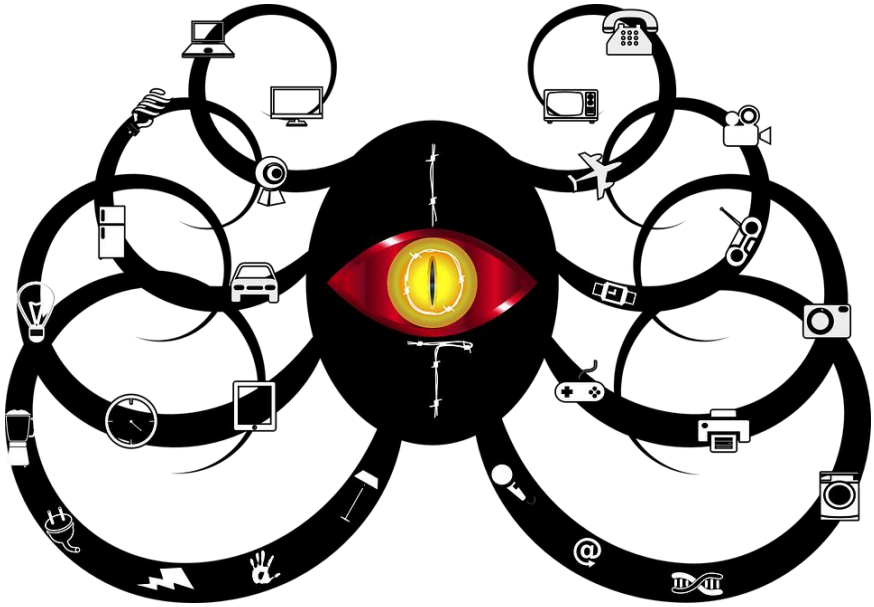
Mass surveillance and the European Courts



A long awaited judgment by the Court of Justice of the European Union (CJEU) published on 26 July 2017 became the most recent addition to a row of judicial criteria that regulate transfers of personal data from the private sector to law enforcement authorities for purposes of mass surveillance. The judgment reaffirmed the aligned positions of the CJEU and the European Court of Human Rights on the strict necessity test required for such transfers, as discussed in this CiTiP blogpost. However, what are the threats these courts aim to confront and how efficiently have they done so?

Mass surveillance and risks

Mass surveillance is distinguished from targeted surveillance as it relates to large groups of people or even entire populations. It affects individuals that are not clearly defined in advance and may not be connected to a specific crime in the first place. In that way, mass surveillance is widely employed by security actors worldwide as a preventive measure, part of an emerging policing strategy and mentality of 'nice-to-have' intelligence. In other words, preventive policing aims at preventing crime through the creation of large databases with as much information as possible in order to generate useful and reliable correlations and ultimately to identify suspects.

Vast quantities of personal data accumulate daily in the hands of businesses, organisations and the private sector in general, forming a pool of information that Member States aspire to dive into. Currently, European and national legal instruments impose on the private sector the obligation to collect and retain, in the name of the fight against terrorism, personal data regarding financial transactions, air-traveling information and electronic communications metadata so that law enforcement authorities of the Member States and of third countries can access and use those data. However, these practices of mass surveillance present numerous risks to citizens' fundamental rights and to society as a whole.

To start with, mass surveillance practices are based on the collection of everyday data from individuals embarking on their everyday activities and can therefore diffuse a feeling of constantly being surveyed

and assessed. Such feeling of constant control may have deep repercussions to individual autonomy and privacy as well as the trust of citizens towards their governments. Additionally, they provide law enforcement authorities with the possibility to acquire a detailed profile of private aspects of citizens' lives and as such, the risk of abuse intensifies.

Indeed, mass surveillance programmes risk illegally interfering with fundamental rights, such as the right to a fair trial, the right to privacy and the right to protection of personal data. In the context of this collect-it-all mentality of preventive policing, information is aggregated to be used potentially as evidence before a crime is even committed. Individuals are quite often unknowingly surveyed before they, if ever, commit any crime and as such they lose their right not to incriminate themselves. It is also practically impossible for them to contest any conclusion about their future potential behaviour deriving from this preventive practices of mass surveillance. Moreover, such measures entail an undifferentiated and generalised access to personal data of all citizens without them having presented or being linked to a threat to national or public security. In that way, mass surveillance practices are not strictly necessary for the purpose of fighting serious crime and safeguarding security and thus unlawfully infringe the fundamental rights to privacy and data protection.

What did the Courts say?

In response to these risks, the two highest Courts of Europe – the CJEU and the ECtHR – have taken a strong and aligned stand in favour of the fundamental rights to privacy and to data protection through a series of judgments, namely in the cases Digital Rights Ireland, Schrems, Tele2 Sverige and the EU-Canada PNR Agreement before the CJEU and Zakharov and Szabó before the ECtHR . Both courts stated that any such measure of mass surveillance must be foreseeable and proportionate in order to be lawful. As such, the legal instruments imposing such measures must be clear with regard the circumstances under which data are being transferred from the private sector to law enforcement authorities. Furthermore, they must provide for objective criteria concerning the selection of data to be transferred as well as appropriate safeguards for the access, use, retention and erasure of the data by law enforcement authorities. Supervisory control by an independent body is of outmost importance and individuals should be notified when they are subject to such measure as well as be given the opportunity to seek effective remedies.

These judgments have been praised for the protective shield they offer individuals and their rights to privacy and to data protection but they have also raised some questions. However, as the Courts attempt to find a compromise between mass surveillance and fundamental rights by providing for the conditions under which mass surveillance may be compliant with fundamental rights, some scholars have criticised the Courts for not denouncing mass surveillance practices in principle while others have questioned the practical enforceability of this set of criteria. Indeed, most legal instruments imposing such measures currently will not be able to meet this high threshold and will thus have to be reviewed. But will this threshold be maintained as high?

The latest judgment by the CJEU (EU-Canada PNR Agreement) adopted a less protective position by allowing for the data of all air passengers indiscriminately to be accessed and processed by the competent authorities. In particular, it simply accepted without any counterargument that access to all of this data is necessary, as, according to the Court, they are "*intended to identify the risk to public security that persons, who are not, at that stage, known to the competent services, may potentially present, and who may, on account of that risk, be subject to further examination".* This is the first time one of the two courts

comments on preventive policing strategies and automated decision making based on mass quantities of data. Even though the Court refers to the need for accuracy and to the right to non-discrimination, it nonetheless offers no further elaboration on the matter. Indeed, what seems to be missing in the reasoning of these rulings is an empirical discussion around investigatory techniques and methods of mass surveillance. Apart from minor exceptions, there is no reference on the actual necessity, efficiency and success rate of 'nice-to-have' intelligence in prevention and detection of crime.

Concluding, while the Courts seem to have addressed most of the risks mass surveillance practices present, it still remains to be seen whether the appropriate balance has been struck.

Categories: Privacy & Data Protection, Security & Crime

Keywords: mass surveillance, private-to-law-enforcement data transfers, preventive policing, European case law,